European Commission

JRC TECHNICAL REPORTS

DSRC CAN INTERFACE SPECIFICATION for the Smart Tachograph application

Gianmarco Baldini

Joint Research Centre

EUR 30244 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Gianmarco Baldini
Address: Via Enrico Fermi 2749, 21027, Ispra (VA)
Email: gianmarco.baldini@ec.europa.eu
Tel.: +39 0332 78 6618

EU Science Hub
https://ec.europa.eu/jrc

JRC120796

EUR 30244 EN

PDF	ISBN 978-92-76-19415-6	ISSN 1831-9424	doi:10.2760/07004
Print	ISBN 978-92-76-19414-9	ISSN 1018-5593	doi:10.2760/128824

Luxembourg: Publications Office of the European Union 2020

How to cite this report: Gianmarco Baldini, DSRC CAN Interface Specification for the Smart Tachograph application, EUR 30244 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19415-6, doi:10.2760/07004, JRC120796.

Contents

Acknowledgements

This technical report is based on the technical specification details an implementation of the DSRC-CAN interface and communication protocol based on the SAE J1939 standard between the Vehicle Unit and a CAN based DSRC module in a Smart Tachograph System. The technical specification has been defined by the tachograph manufacturers Stoneridge, Continental and Intellic with the technical support of the Joint Research Centre of the European Commission and the vehicle manufactures via the HDEI (Heavy Truck Electronic Interface) working group.

Gianmarco Baldini from EC JRC has only inserted the content from the technical specification in the format of a JRC Technical report to complement the Smart Tachograph regulation: European Commission, Commission implementing regulation (EU) 2016/799 of 18 march 2016 implementing regulation (eu) no 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, 2016.

Authors

Gianmarco Baldini (on behalf of the HDEI working group)

Executive Summary

This document defines the protocol between the Vehicle Unit (VU) and the DSRC-VU module in the Smart Tachograph application defined in the Commission implementing regulation (EU) 2016/799 of 18 march 2016 implementing regulation (EU) no 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components.

The high level definition of the protocol (application layer) between the VU and the DSRC-VU module in the Smart Tachograph application is provided in Appendix 14 of regulation (EU) 2016/799. In Appendix 14, different options are possible for the choice of the lower layers of the protocol (e.g., transport layer) to be adopted.

This document describes the specific implementation of the protocol on the basis of the standard SAE J1939 standard between the VU and a CAN based DSRC module. SAE J1939 defines five layers in the seven-layer OSI network model, and this includes the Controller Area Network (CAN) ISO 11898 specification (using only the 29-bit/"extended" identifier) for the physical and data-link layers.

In this context, this document complements regulation (EU) 2016/799 for the specific implementation of the VU to DSRC-VU protocol on the basis of SAE J1939.

1 Document Scope

This document specifies the CAN protocol based on the [SAE J1939] standard between a Smart Tachograph and a DSRC-VU module, implementing the suggested Application Protocol defined in Annex 1C Appendix 14.

2 Relevant Documents

Reference Id	Title
[Annex1C]	Commission implementing regulation (EU) 2016/799 of 18 march 2016 implementing regulation (EU) no 165/2014 of the European Parliament and of the Council laying down the requirements for the construction, testing, installation, operation and repair of tachographs and their components, 2016. http://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 32016R0799
[Annex1C Amendment]	Ares(2017) 5184151. Draft Implementing regulation.
[Annex1C Appendix 1]	Appendix 1. Data Dictionary of [Annex1C].
[Annex1C Appendix 11]	Appendix 11. Common Security Mechanisms of [Annex1C].
[Annex1C Appendix 14]	Appendix 14. Remote Communication Function of [Annex1C].
[ISO 16844-4]	ISO 16844-4:2015 Road vehicles – Tachograph systems – Part 4 : CAN Interface
[ISO 8825-2]	ISO/IEC 8825-2:2015 Information technology - ASN.1 encoding rules – Part 2: Specification of Packed Encoding Rules (PER). 2015.
[ISO 8825-7]	ISO/IEC 8825-7:2015 Information technology - ASN.1 encoding rules – Part 7: Specification of Octet Encoding Rules (OER). 2015.
[SAE J1939]	Recommended Practice for a Serial Control and Communications Vehicle Network
[SAE J1939-21]	SAE J1939-21:MAR2016, Data Link Layer

3 Document Revision History

Rev: 0.1 Date of issue: 2020-04-28 Issued by EC DG JRC on the basis of the document prepared by Smart Tachograph stakeholders and coordinated by Stoneridge (coordinator: Lars Bodin)
Version for review.

Rev: 1.0 Date of issue: 2020-05-12 Issued by EC DG JRC on the basis of the review provided by stakeholders.
Final Version for publication.

4 General

[Annex 1C Appendix 14] defines the communication between a VU-RTM unit inside a Smart Tachograph (SM) and a Remote Early Detection Communication Reader (REDCR) as described in Figure 1.

One potential solution to this purpose is to use an external DSRC module (DSRC-VU) connected by a CAN bus using a communication protocol based on SAE J1939 defined in [SAE J1939-21]. A suggested application protocol and data transfer between VU-RTM and DSRC-VU is defined in [Annex 1C Appendix 14].

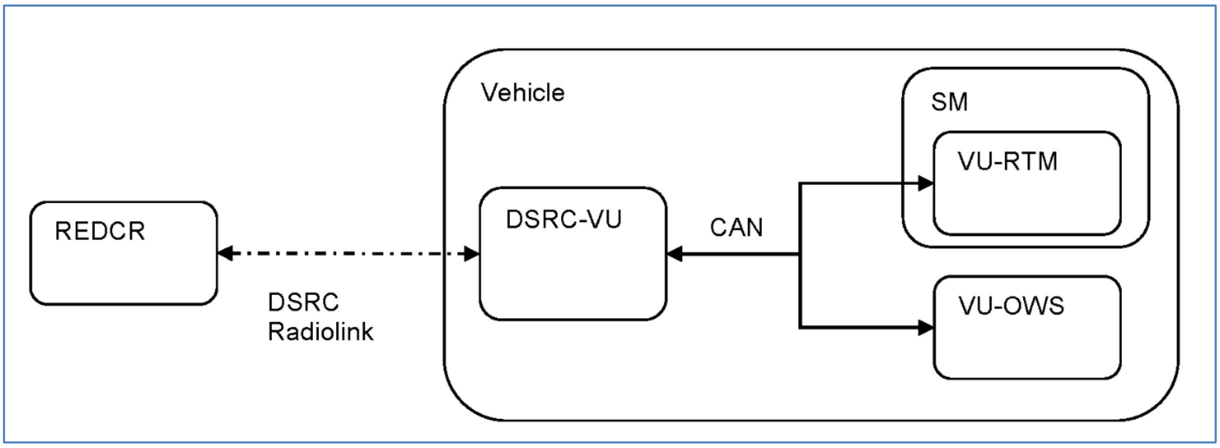

Figure 1 Communication between a VU-RTM unit inside a Smart Tachograph (ST) and a Remote Early Detection Communication Reader (REDCR)

Note: The implementation of a connection between the DSRC-VU and the VU-OWS is dependent on the future implementation of Directive (EU) 2017/719 and it is not addressed in this document.

This document specifies the CAN interface for the communication between digital tachographs and DSRC modules (DSRC-VU), including the attributes needed to implement the Parameter Group (PG) content. The application protocol and the physical layer are only referenced in the corresponding standards. The referenced standards for each layer are listed in the following Table 1.

Layer	Referenced Standard	Main Chapter
Application Layer	[Annex1C Appendix 11]	13ff Security for Remote Communication over DSRC
	[Annex1C Appendix 14]	5.6.2 Application Protocol
	[ISO 8825-2]	All
Transport Layer	[SAE J1939-21]	5.10 Transport Protocol Function
Data Link Layer	[ISO 16844-4]	6 Data link layer application requirements
Physical Layer	[ISO 16844-4]	5 Physical layer application requirements

Table 1 Layers and referenced standards in DSRC communication.

5 Physical Layer

The physical layer for the DSRC CAN communication is defined in ISO 16844-4 Road vehicles- Tachograph systems- Part 4: CAN Interface [ISO 16844-4].

6 Transport Layer

The transport layer defined for the communication between DSRC-VU and VU-RTM or VU-OWS is the ‘Transport Protocol Function’, defined in [SAE J1939-21], for Parameter Groups which has 9 or more data bytes to transfer. The ‘Transport Protocol Function’ has the capability to communicate the data itself in a series of CAN Data Frames (packets) containing the packetized data. Additionally, the Transport Protocol Function provides flow control and handshaking capabilities for destination specific transfers.

A Parameter Group defined as multi-packet capable, having fewer than 9 data bytes to transfer in a specific instance, shall be sent in a single CAN Data Frame with the DLC set to 8.

The ‘Transport Protocol Function’, between precisely two ECUs, allows a transmission of messages of arbitrary length up to 1785 bytes. The data flow for one PG can be bidirectional and is controlled by a handshake between sender and receiver ECU. The handshake consists of four dedicated message identifiers RTS, CTS, EndOfMsgACK and Conn_Abort, which are sent in connection management (TP.CM) messages. In case of error, the handshake mechanism allows a retransmission of communication subsequence without a complete repetition of the whole PG. In addition, the reception of a PG is confirmed by the receiving ECU.

The protocol is partly defined in [ISO 16844-4] and in any detail in [SAE J1939-21].

6.1 SAE J1939 Transport Protocol Function

The ‘Transport Protocol Function’, between precisely two ECUs, allows a transmission of messages of arbitrary length up to 1785 bytes. The data flow for one PG can be bidirectional and is controlled by a handshake between sender and receiver ECU. The handshake consists of four dedicated message identifiers RTS, CTS, EndOfMsgACK and Conn_Abort, which is sent in connection management (TP.CM) messages. In case of error, the handshake mechanism allows a retransmission of communication subsequence without a complete repetition of the whole PG. In addition, the reception of a PG is confirmed by the receiving ECU.

The protocol is partly defined in [ISO 16844-4] and in any detail in [SAE J1939-21].

Note: the “ProprietaryA” PGN number (61184) will be used.

6.2 CAN node address

The CAN node address of a Smart Tachograph is defined as 0xEEh (238dec) in [ISO 16844-4]. The fixed address for the DSRC-VU module will be configurable to support different manufacturer needs.

ECU	Address	Comment
Smart Tachograph	0xEEh	
DSRC-VU	0xXXh	Shall be configurable in DSRC-VU and VU

Table 2 CAN node address

6.3 DSRC CAN Parameter Group Number

6.3.1 DSRC_Communication

Name	Value	Comment
DSRC_Communication	61184 (00EF00h)	The Parameter Group Number (PGN) is from J1939-21.

Table 3 DSRC_Communication Parameter Group Number

DSRC_Communication will be used for sending DSRC command identity, application link identity and possibly including additional data related to the specific command (e.g. RCDT Data in SendData command).

Attribute	Value
Transmission Repetition Rate	On request
Data Length	Variable, 2 to 1785 bytes
Extended Data Page	0
Data Page	0
PDU Format	239
PDU Specific	Destination Address (DA)
Default Priority	6
PGN	61184_{10}/$00EF00_{16}$

Table 4 DSRC_Communication attribute specification

7 Application Layer

The application layer, for the DSRC_Communication PG, consists of three pairs of commands for initializing an application link, cyclic exchange of RTM/OWS data and for termination of the application link.

For application management the two command pairs “Initialization Request/Response” and “Termination Request/Response” are used. The “SendData” and “Acknowledgement of data” is used for cyclic transmission of application data for RTM and OWS. The application data in the “SendData” command is encrypted and signed before transmission according to chapter 13. “Security for Remote Communication over DSRC” of [Annex 1C Appendix 11].

Command	Direction	Payload defined in[Annex 1C Appendix 14]
Initialization Request	VU->DSRC-VU	RCDT-Communication Link Initialization - Request
Initialization Response	VU<-DSRC-VU	RCDT-Communication Link Initialization - Response
Send Data	VU->DSRC-VU	RCDT- Send Data (for RTM or OWS)
Acknowledgment of the data	VU<-DSRC-VU	RCDT Data Acknowledgment
Termination Request	VU->DSRC-VU	RCDT-Communication Link Termination - Request
Termination Response	VU<-DSRC-VU	RCDT-Communication Link Termination - Response

Table 5 Application Commands

7.1 DSRC_Communication Parameter Group

The content of the DSRC_Communication PG is divided in two parts. The first part defines the command header and the second part contains a variable length of bytes depending on type of command, i.e. either the answer in a response command or the payload of the RTM or OWS data, in a send data request:

Header
Answer or RTM / OWS Payload

7.1.1 DSRC_Communication CAN Header

The Header consists of two parts. The DSRC command transmitted in the message and an identifier specifying the application used in the message. Possible choices are RTM, OWS or further applications defined in the future.

Byte pos	Bit pos	Parameter	Remarks
1		Command_ID	See Table 7
2		Link_ID	See Table 8

Table 6 DSRC_Communication header specification

Attribute	Value
Data length	1 byte
Resolution	1/bit
Operating range	0 – LinkInitializationRequest 1 – LinkInitializationResponse 2 – SendData 3 – AcknowledgeData 4 – LinkTerminationRequest 5 – LinkTerminationResponse 6 to 255 reserved for further usage

Table 7 Command_ID specification

Attribute	Value
Data length	1 byte
Resolution	1/bit
Operating range	0 – RemoteTachographMonitoring 1 – OnboardWeighingSystem 2 to 255 reserved for further usage

Table 8 Link_ID specification

7.1.2 DSRC_Communication Payload

The payload for the DSRC_Communication PG varies in size according to the application and command specified in the header. Size and content are defined in chapter 8.2.

The plain text DSRC payload is either the RTM or the OWS data. The OWS data is supported for future use only. The plain text TachographPayload (and OwsPayload) shall be encoded using OER (Octet Encoding Rules) defined in ISO/IEC 8825-7, Rec. ITU-T X.696 (according to update of DSC_43 in Annex 1C Amendment, see [Annex1C Amendment]). See ASN.1 specification and examples of encoding of the plain text TachographPayload in chapter 10.

All other data, including the RCDTData, in the DSRC-REDCR transactions shall be encoded using UPER (Unaligned Packet Encoding Rules). See examples of RCDTData encoding in chapter 10.5..

7.2 Application protocol

For ASN.1 definition of the application protocol, see chapter 10.1.

7.2.1 Initialization of the communication link – Request

The initialization of the requested application link shall be done at the start of the engine/when VU is switched on (IGNITION_ON), after the VU has been activated and calibrated. The Link_ID attribute is used in all further messages until the communication is terminated or the communication is restarted after IGNITION ON. If the given application link is already used by another ongoing communication, the DSRC-VU shall answer with a negative acknowledgement in the LinkInitializationResponse message.

The initialization request should be successfully finished with a positive acknowledgement before the cyclic communication starts. In case of no response from the DSRC-VU, the request shall be restarted after a 10 second timeout.

Byte pos	Parameter	Value	Type
1	Command_ID	0x00	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)

Table 9 LinkInitializationRequest specification

7.2.2 Initialization of the communication link – Response

LinkInitializationResponse command is used by the DSRC-VU to provide the response of the request to initialize the application link. The command shall be sent by the DSRC-VU to the VU. The command provides the result of the initialization. If a Link_ID is already in use by a VU, the DSRC-VU shall answer negatively to any other VU trying to use this Link_ID.

Byte pos	Parameter	Value	Type
1	Command_ID	0x01	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3	Answer	0x01 (Success) 0x00 (Failure)	INTEGER (0..255)

Table 10 LinkInitializationResponse specification

7.2.3 Send Data

SendData command is used by the VU to send the signed RCDTData (i.e., the remote communication Data) to the DSRC-VU. The data shall be sent every 60 seconds. The Link_ID is used to ensure that the appropriate application link is used. Any message with a false Link_ID or without a previous link established should be rejected by a negative Acknowledgement. Only one ongoing transaction is allowed per each specific application link (Link_ID). If the VU has not received an Acknowledgement within 15 seconds, it shall abort the current transmission.

Byte pos	Parameter	Value	Type
1	Command_ID	0x02	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3 to 1785 (variable)	RCDTData	See chapter 8.1.2 and chapter 10.5	See 8.1.2

Table 11 SendData specification

7.2.4 Acknowledgment of the data

AcknowledgeData is sent by the DSRC-VU to provide the feedback to the VU on the reception of the data from a SendData command. The DSRC-VU shall acknowledge within 10 seconds from received SendData. If a VU receives more than three subsequent answers equal to 0 or if the VU does not receive an AcknowledgeData, the VU shall generate and record an event ('62'H Remote Communication Facility communication fault). The VU should then terminate and re-initialize the specific link before sending data again. If a Link_ID is already in use by a VU, the DSRC-VU shall answer with negative acknowledgement to any other VU trying to use this Link_ID.

Byte pos	Parameter	Value	Type
1	Command_ID	0x03	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3	Answer	0x01(Success) 0x00 (Failure)	INTEGER (0..255)

Table 12 AcknowledgeData specification

7.2.5 Termination of the communication link – Request

LinkTerminationRequest shall be sent by the VU to DSRC-VU to terminate a link for a specific application link (Link_ID). The DSRC-VU shall positively confirm the termination, regardless if the specific link is initialized or not. In case of no response from the DSRC-VU within 10 seconds, the VU shall regard the link as successfully terminated.

Byte pos	Parameter	Value	Type
1	Command_ID	0x04	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)

Table 13 LinkTerminationRequest specification

7.2.6 Termination of the communication link – Response

Byte pos	Parameter	Value	Type
1	Command_ID	0x05	INTEGER (0..255)
2	Link_ID	See Table 8	INTEGER (0..255)
3	Answer	0x01(Success) 0x00 (Failure)	INTEGER (0..255)

Table 14 LinkTerminationResponse specification

8 List of Abbreviations

CAN	Controller Area network
Conn_Abort	Connection Abort. See [SAE J1939-21] CTS
DSRC	Dedicated Short Range Communications
ECU	Electronic Control Unit
EndOfMsgACK	End Of Message Acknowledgement. See [SAE J1939-21]
HDEI	Heavy Truck Electronic Interface
OER	Octet Encoding Rules
OWS	On-board Weighing System
PER	Packed Encoding Rules
PG	Parameters Group
PGN	Parameter Group Number
REDCR	Remote Early Detection Communication Reader
RCDT	Remote Communication Digital Tachograph
RTM	Remote Tachograph Monitoring
RTS	Request To Send. See [SAE J1939-21] SAE
SM	Smart Tachograph
VU	Vehicle Unit
VU-OWS	Vehicle Unit – Onboard Weighing System

9 List of Figures

10 List of Tables

Annexes

Annex 1 Example of CAN Sequence

Assumptions:

Tacho Source Address=0xEE DSRC

Source Address=0x7E

DSRC_Communication PGN = 0x00EF00

DSRC← →Tacho

At ignition ON:

←REQUEST:	DSRC_Com	PGN: 0x18EF7EEE len:8 data: 00 00 FF FF FF FF FF FF
		(LinkInitializationRequest, RTM)
→RESPONSE:	DSRC_Com	PGN: 0x18EFEE7E len:8 data: 01 00 01 FF FF FF FF FF
		(LinkInitializationResponse, RTM, ok)

Each 60 seconds:

←COMMAND:	TP.CM_RTS	PGN: 0x18EC7EEE len:8 data: 10 LL LL PP FF 00 EF 00
		(RTS, LLLL bytes, #PP, PGN=00EF00)
→RESPONSE:	TP.CM_CTS	PGN: 0x18ECEE7E len:8 data: 11 PP 01 FF FF 00 EF 00
		(CTS, packet sup PP, next 01)
←COMMAND:	TP.DT	PGN: 0x18EB7EEE len:8 data: 01 02 00 TT TT TT TT TT
		(SeqN=01, SendData, RTM, RCDT=TT)
←COMMAND:	TP.DT	PGN: 0x18EB7EEE len:8 data: 02 TT TT TT TT TT TT TT
		(SeqN=02, RCDT=TT)
…		
←COMMAND:	TP.DT	PGN: 0x18EB7EEE len:8 data: PP TT TT TT TT TT TT TT
		(SeqN=PP, RCDT=TT (fill with 0xFF))
→RESPONSE:	TP.CM_EOMA	PGN: 0x18ECEE7E len:8 data: 13 LL LL PP FF 00 EF 00
		(EndOfMsgACK, LLLL bytes, packets PP)
→RESPONSE:	DSRC_Com	PGN: 0x18EFEE7E len:8 data: 03 00 01 FF FF FF FF FF
		(AcknowledgeData, RTM, ok)

At restart:

←REQUEST:	DSRC_Com	PGN: 0x18EF7EEE len:8 data: 04 00 FF FF FF FF FF FF
		(LinkTerminationRequest, RTM)
→RESPONSE:	DSRC_Com	PGN: 0x18EFEE7E len:8 data: 05 00 01 FF FF FF FF FF
		(LinkTerminationResponse, RTM, ok)

Annex 2 ASN.1 Definitions and Data Examples

Remote-Communication-DT-Protocol Definition

-- Annex 1C DSC_73

-- The value range of link Identifier is limited to 0..255 in this proposed document while it is specified as full INTEGER in [Annex1C] (Appendix 14 DSC_73). The proposal in this document should not be considered to be in conflict with [Annex1C], but it is a recommendation.

```
Remote-Communication-DT-Protocol DEFINITIONS ::= BEGIN

RCDT-Command ::= SEQUENCE
{
unused INTEGER(0..31), -- waste 5 bit payload RCDT-Payload
}

RCDT-Payload ::= CHOICE
{
link-Initialization-Request [0] RCDT-Communication-Link-Initialization-Request,
link-Initialization-Response [1] RCDT-Communication-Link-Initialization-Response,
send-Data [2] RCDT-Send-Data,
data-Acknowledgment [3] RCDT-Data-Acknowledgment,
link-Termination-Request [4] RCDT-Communication-Link-Termination-Request,
link-Termination-Response [5] RCDT-Communication-Link-Termination-Response
}

RCDT-Communication-Link-Initialization-Request ::= SEQUENCE
{
linkIdentifier INTEGER(0..255) -- 0x00 = RTM, 0x01 = OWS, 0x02..0xFF reserved for future use
}

RCDT-Communication-Link-Initialization-Response ::= SEQUENCE
{
linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02..0xFF reserved for future use
answer INTEGER(0..255) -- Link initialization accepted: 1 (Success), 0 (Failure)
}

RCDT-Send-Data ::= SEQUENCE
{
linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02..0xFF reserved for future use
rCDTData SignedTachographPayload
}

RCDT-Data-Acknowledgment ::= SEQUENCE
{
linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02..0xFF reserved for future use
answer INTEGER(0..255) -- rCDTData correctly received: 1 (Success), 0 (Failure)
}

RCDT-Communication-Link-Termination-Request ::= SEQUENCE
{
linkIdentifier INTEGER(0..255) -- 0x00 = RTM, 0x01 = OWS, 0x02..0xFF reserved for future use
}
```

```
RCDT-Communication-Link-Termination-Response ::= SEQUENCE
{
linkIdentifier INTEGER(0..255), -- 0x00 = RTM, 0x01 = OWS, 0x02..0xFF reserved for future use
answer INTEGER(0..255) -- Link termination accepted: 1 (Success), 0 (Failure)
}
-- Annex 1C, DSC_38 The payload (RTM data) consists of the concatenation of
-- 1. encryptedTachographPayload data, which is the encryption of the TachographPayload
-- defined in ASN.1 in section 5.4.5. The method of encryption is described in Appendix 11
-- 2. dSRCSecurityData, specified in Appendix 11.
-- The SignedTachographPayload corresponds to the payload (RTM data).
-- In the DSRC communication the SignedTachographPayload is the RtmData as per ASN.1
-- definition of DSC_40. SignedTachographPayload ::= RtmData
RtmData ::= SEQUENCE
{
encryptedTachographPayload OCTET STRING (SIZE(67))
        (CONSTRAINED BY { -- calculated encrypting TachographPayload as per Appendix 11 --}),
        dSRCSecurityData OCTET STRING
}
END
```

Tachograh Payload Definition

```
Tachograph-Payload DEFINITIONS AUTOMATIC TAGS ::= BEGIN

TachographPayload ::= SEQUENCE {
tp15638VehicleRegistrationPlate LPN, -- Vehicle Registration Plate as per EN 15509.
-- In this application, LPN is fixed to 17 bytes long, according to Annex 1C, DSC_41 and DSC_43.
tp15638SpeedingEvent            BOOLEAN, -- l = Irregularities in speed
tp15638DrivingWithoutValidCard  BOOLEAN, -- l = Invalid card usage
tp15638DriverCard               BOOLEAN, -- 0 = Indicates a valid driver card
tp15638CardInsertion            BOOLEAN, -- 1 = Card insertion while driving
tp15638MotionDataError          BOOLEAN, -- 1 = Motion data error
tp15638VehicleMotionConflict    BOOLEAN, -- 1 = Motion conflict
tp156382ndDriverCard            BOOLEAN, -- 1 = Second driver card inserted
tp15638CurrentActivityDriving   BOOLEAN, -- 1 = other activity selected -- 0 = driving selected
tp15638LastSessionClosed        BOOLEAN, -- l = improperly, 0 = properly closed
tp15638PowerSupplyInterruption  INTEGER(0..127), -- Supply interrupts in the last 10 days
tp15638SensorFault              INTEGER(0..255), -- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex lC.
tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last -- time adjustment
tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous -- calibration data
tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
tp15638CurrentSpeed             INTEGER(0..255), -- Last current recorded speed
tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record
}

-- LPN, Vehicle Registration Plate as per EN 15509
-- EN 15509 refers to ISO 14906, the definition is copied from ISO_14906_2011.pdf
-- According to Annex 1C, DSC_41 and DSC_43, this LPN shall be fixed to 17 bytes long
LPN ::= SEQUENCE { countryCode CountryCode, alphabetIndicator ENUMERATED {
latinAlphabetNo1 (1), -- OER encoded as '0000 0001'B
latinAlphabetNo2 (2), -- OER encoded as '0000 0010'B
latinAlphabetNo3 (3),
latinAlphabetNo4 (4),
latinCyrillicAlphabet (5),
latinArabicAlphabet (6),
latinGreekAlphabet (7),
latinHebrewAlphabet (8),
latinAlphabetNo5 (9),
latinAlphabetNo6 (10),
twoOctetBMP (11),
fourOctetCanonical (12),
reservedForUse1 (13),
reservedForUse2 (14),
reservedForUse3 (15),
reservedForUse4 (16),
reservedForUse5 (17),
reservedForUse6 (18),
reservedForUse7 (19),
reservedForUse8 (20),
reservedForUse9 (21),
reservedForUse10 (22),
reservedForUse11 (23),
reservedForUse12 (24),
reservedForUse13 (25),
reservedForUse14 (26),
reservedForUse15 (27),
reservedForUse16 (28),
reservedForUse17 (29),
reservedForUse18 (30),
reservedForUse19 (31),
reservedForUse20 (32),
reservedForUse21 (33)
} -- latinAlphabetNo1 recommended -- ,
-- refer to Annex E for conversion from LatinAlphabetNo2
-- and LatinAlphabetNo5 to Latin AlphabetNo1
licencePlateNumber OCTET STRING (SIZE(14))
-- Note: The licencePlateNumber shall be fixed to 14 bytes and equal to the
VehicleRegNumber in Annex 1C/ISO16844-7, i.e. 13 bytes long + one padding byte (zeros).
No length determinant for the licencePlateNumber is needed since it is fixed 14 bytes long.
}
-- Below imported data from ISO 14816's ASN.1 module
CountryCode ::= BIT STRING(SIZE(10)) -- Value assignment is done in accordance with ISO
3166-1 and by using the ITA.2 alphabet.
END
```

Example of Tachograph Payload Raw Data in ASN.1 Notation

```
tpl TachographPayload ::=
{
tp15638VehicleRegistrationPlate
{
countryCode '10010 01000'B, -- Sweden
alphabetIndicator latinAlphabetNo1,
licencePlateNumber '56 53 2D 41 42 20 31 32 33 34 00 00 00 00'H -- VS-AB 1234
},
tp15638SpeedingEvent TRUE,
tp15638DrivingWithoutValidCard FALSE,
tp15638DriverCard TRUE,
tp15638CardInsertion FALSE,
tp15638MotionDataError TRUE,
tp15638VehicleMotionConflict TRUE,
tp156382ndDriverCard FALSE,
tp15638CurrentActivityDriving FALSE,
tp15638LastSessionClosed TRUE,
tp15638PowerSupplyInterruption 4,
tp15638SensorFault 164,
tp15638TimeAdjustment 1483272000, -- (GMT): Sunday, January 1, 2017 12:00:00 PM
tp15638LatestBreachAttempt 255, -- default value 0x000000FF
tp15638LastCalibrationData 1483272300, -- (GMT): Sunday, January 1, 2017 12:05:00 PM
tp15638PrevCalibrationData 0, -- default for no preceding calibration
tp15638DateTachoConnected 1484481600, -- (GMT): Sunday, January 15, 2017 12:00:00 PM
tp15638CurrentSpeed 79,
tp15638Timestamp 1503481476 -- (GMT): Wednesday, August 23, 2017 9:44:36 AM
}
```

Example of OER encoded tpl (TachographPayload)

92000156 532D4142 20313233 34000000 00FF00FF 00FFFF00 00FF04A4 5868EF40
000000FF 5868F06C 00000000 587B6440 4F599D4E 84

92 00 countryCode
01 alphabetIndicator
56 53 2D 41 42 20 31 32 33 34 00 00 00 00 licencePlateNumber
FF tp15638SpeedingEvent
00 tp15638DrivingWithoutValidCard
FF tp15638DriverCard
00 tp15638CardInsertion
FF tp15638MotionDataError
FF tp15638VehicleMotionConflict
00 tp156382ndDriverCard
00 tp15638CurrentActivityDriving
FF tp15638LastSessionClosed
04 tp15638PowerSupplyInterruption
A4 tp15638SensorFault
58 68 EF 40 tp15638TimeAdjustment
00 00 00 FF tp15638LatestBreachAttempt
58 68 F0 6C tp15638LastCalibrationData
00 00 00 00 tp15638PrevCalibrationData
58 7B 64 40 tp15638DateTachoConnected
4F tp15638CurrentSpeed
59 9D 4E 84 tp15638Timestamp.

Before the encryption, padding has to be added, with 11 bytes (53+11=64) in order to get a multiple of 16 octets.

UPER Encoded RCDTData

RCDTDATA (RTMData) shall have the following lenghts:

96 octets (for MAC(8)), 100 octets (for MAC(10)) or 104 octets (for MAC(12)).

Example: sendData with length of RCDTData=67+1+28 = 96 octets (MAC(8)), where 67 octets are the encryptedTachographPayload, 1 octet is the length indicator for the following DSRCSecurityData and the 28 octets are the DSRCSecurityData.

I.e. since the DSRCSecurityData is variable, a length indicator is included in the payload.

VU-RTM -> DSRC-VU: 02 00 87 41 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

1C 81 10 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 8E 08 xx xx xx xx xx xx xx xx.

Header	RTM / OWS Payload (hex data)
02 commandID sendData 00 linkIdentifier remoteTachographMonitoring	87 41 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx encryptedTachographPayload **1C** length indicator 81 10 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx dSRCSecurityData (excl MAC) 8E 08 xx xx xx xx xx xx xx xx MAC(8)

Table 15 UPER encoded RCDTData

Annex 3 Context Mark

It should be noted that the context mark example in Annex 1C DSC_48, table 14.9, is incorrectly encoded. According to DSC_43, all DSRC transactions shall be unaligned PER encoded. I.e. the Rtm-ContextMark shall be encoded according to the Table 16 below.

(The octet 16 and 19 has been removed from original Annex 1C DSC_48.)

Octet #	Attribute/Field	Bits in octet	Description
15		0000 0110	No extension, Rtm-ContextMark length = 6
16	Rtm-ContextMark ::= SEQUENCE { standardIdentifier StandardIdentifier }	0000 0101	First octet is 05H, which is its length. Subsequent 5 octets encode the Object Identifier of the supported standard, part, and version. {iso (1) standard (0) Tarv (15638) part9 (9) version1 (1)}
17		0010 1000	
18		1111 1010	
19		0001 0110	
20		0000 1001	
21		0000 0001	

Table 16 Context Mark (UPER encoding)

KJ-NA-30244-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office
of the European Union

doi:10.2760/07004

ISBN 978-92-76-19415-6